Intel® IT Pilot Project

Active Directory* on the Intel® Itanium® Processor Architecture

Active Directory* is a Windows* 2000-based directory service that is the foundation for a broad range of Intranet services in distributed networking environments. At Intel, increased performance demands will likely require significant capacity relief in 2001 and beyond. Active Directory on an Itanium™-based platform is a key component of Intel IT's strategy to provide this

November 2001

Table of Contents

Active Directory* Pilot at Intel®

Active Directory* is a Windows* 2000-based directory service designed for distributed networking environments. It is the foundation for a broad range of intranet services. In early 2000, Intel® began migrating its Windows NT* 4.0 domain infrastructure to Windows 2000 and Active Directory on high-powered Intel® Pentium® III Xeon™ and Pentium® III processor-based platforms. While this new deployment offers many beneficial features and technologies, increased performance demands will likely require significant capacity relief in 2001 and beyond. Active Directory on an Itanium™-based platform is a key component of Intel IT's strategy to provide this relief.

This paper describes Intel IT's Active Directory pilot on an Itanium-based server, including the strategy, system architecture, and results of the pilot.

Goals of the Pilot

In order to prepare for the implementation of an Itanium-based Active Directory infrastructure in 2001, Intel IT conducted an end-user pilot designed to:

- Demonstrate that all aspects of an Itanium-based solution stack are mature enough to support pilot-level service to end-users.
- Demonstrate interoperability between an Itanium-based (64-bit) Active Directory infrastructure and an IA-32 Active Directory infrastructure.
- Illustrate how the flexibility of Active Directory's security permits the execution of a pilot in an isolated *forest* (a collection of domains) while maintaining each pilot participant's access to all resources on the production network.
- Port internally developed Active Directory migration tools to run on the Itanium architecture as native 64-bit components.

Domain Architecture & Strategy

Pilot Domain Configuration

To accurately represent a typical Active Directory implementation, the pilot domain configuration used multiple Itanium-based servers. A 32-bit server was included to demonstrate seamless interoperability between those platforms.

The physical infrastructure supporting Active Directory on the Itanium pilot system consisted of a single Microsoft* Whistler-64 domain, with two prototype Intel Itanium-based servers and one dual-processor Pentium III server acting as domain controllers. The Itanium servers ran Whistler-64 build 2259 and the Pentium III server ran Whistler-32 build 2259 (both pre-Beta 1 builds). All domain controllers were located at Intel's Folsom, CA campus. Pilot participants primarily ran Windows 2000 build 2195 on a variety of desktop and notebook configurations. They were located at Intel facilities in Folsom, CA; Santa Clara, CA; Hillsboro, OR; Phoenix, AZ; and Hudson, MA. For the purpose of this white paper, the pilot domain will be referred to as i*a64.intel.com*.

A secondary benefit of this configuration was extra redundancy for failover of critical services. The 32-bit server was configured such that clients would use it only for authentication and global catalog lookups, and only if the Itanium servers were unavailable. (See the discussion of Active Directory sites for more detail.)

Trust Architecture

An extensive network of trust relationships was established to facilitate the migration of pilot users to the Whistler-64 pilot domain, and to allow the migrated users to continue seamless resource sharing with all other Windows NT 4.0 and Windows 2000 users at Intel.

The trust relationships depicted in Figure 1 show NT 4.0-style NT LAN Manager (NTLM) trusts in both directions (two-way trusts) between the ia64.intel.com domain and all of the account domains. Additionally, all Intel IT-supported Windows NT 4.0 resource domains were configured to trust the ia64.intel.com pilot domain (one-way trust).

The user migration process for the pilot took advantage of the Security IDentifier (SID) history capability introduced in Windows 2000. Therefore, it was not necessary to change the security access control lists on any of the migrated users' files, shares, or applications (for example, Microsoft Exchange* mailbox).

Active Directory Site Model

Since all the domain controllers resided at Intel's Folsom, CA campus, the replication topology was very simple. Furthermore, there were no Active Directory-integrated applications, such as Distributed File System (DFS), that would have required separating the various Intel facilities within Active Directory to contain those client/server interactions to campus LANs. A single Active Directory Site was configured to support the Itanium-based servers and all client workstations.

To support the pilot goal of demonstrating interoperability between Itanium-based servers and IA-32 servers, a Pentium III (32-bit) server was included as a replicated instance of the pilot domain. To minimize the possibility that a pilot client would select the 32-bit server for authentication and global catalog queries, a second Active Directory site was created and the 32-bit server was placed in that site. Clients would select this server only after unsuccessfully attempting to locate both Itanium-based servers. All logons were tracked during the pilot and only very rarely did clients log on using the 32-bit server. The following cases account for the vast majority of 32-bit logon occurrences:

- Some client participants had secondary Windows NT 4.0 or Windows 95/98 clients that randomly selected a domain controller without regard to site topology. In these cases, there was a 33% chance that the client would authenticate using the 32-bit server.
- In some cases, pilot participants who did not carry out the migration procedure properly would log on to a user account in the ia64.intel.com domain but would still be using a client PC that was in another domain. In these cases, there was a 33% chance that the client would authenticate using the 32-bit server.
- In one case, a network infrastructure outage took both Itanium-based servers offline for a short period.

DNS Architecture

The Domain Name System (DNS) infrastructure supporting the ia64.intel.com domain ran Microsoft's Active Directory-integrated Dynamic DNS on domain controllers in a production Windows 2000 domain.

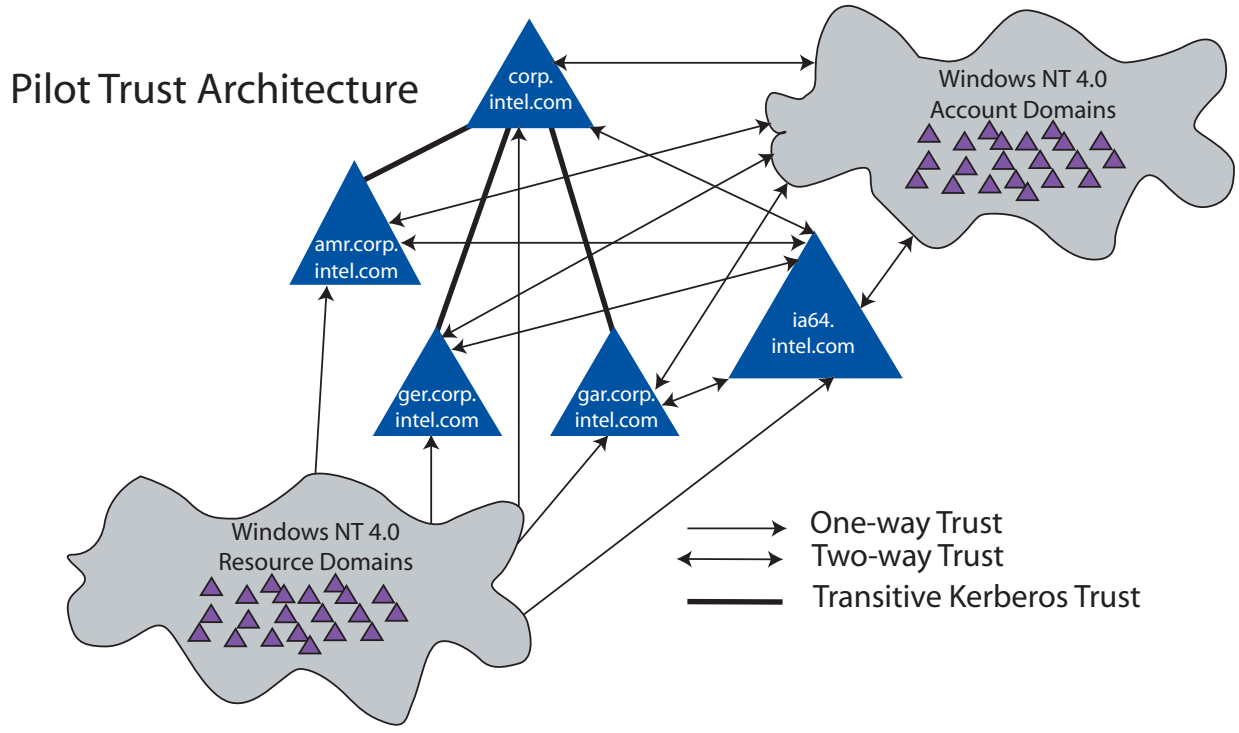

Figure 1. Pilot Trust Architecture

Pilot Results

All pilot goals were achieved, demonstrating that Intel's Itanium architecture is a powerful, strategic platform for Active Directory services.

Goal 1 – Maturity of solution stack:

Demonstrate that all aspects of an Itanium-based solution stack are mature enough to support pilot-level service to end-users.

Even with prototype servers and pre-Beta versions of Microsoft's Whistler operating system, all pilot participants were able to reliably use the ia64.intel.com domain for all of their Active Directory security services. Pilot participants were able to log on to the corporate network and access production resources, such as e-mail, enterprise applications, and shared file and print services. The Itanium-based directory services were available 24x7 for four weeks; the only outage was minor and was invisible to the users.

Goal 2 – Interoperability:

Demonstrate interoperability between an Itanium-processor-based Active Directory infrastructure and an IA-32 Active Directory infrastructure.

Active Directory content was successfully replicated among domain controllers in the pilot domain, including both Itanium-based servers and the 32-bit Pentium III server. In addition, pilot participants were able to utilize Active Directory services transparently and without difficulty from their 32-bit Windows 2000 clients. Security credentials were migrated from Intel's production IA-32 Active Directory to an Itanium-based domain controller. The underlying API that executed this security transfer (Microsoft's dsAddSidHistory function) was invoked successfully from both the 32-bit and 64-bit environments, using Intel's internally developed group synchronization and user migration tools.

PILOT TIMEFRAME

Week	Action	Result
1-2	Identify and recruit pilot users.	Targeted pilot users: Intel IT employees already in a production Active Directory environment; Intel Active Directory employees; and Intel Sales & Marketing (SMG) employees.
3	Move Windows NT4 pilot users into the production Active Directory.	SMG pilot users not in the production Active Directory were migrated using an internally developed migration process. All migrations were successful. The reasons for moving the Windows NT4 users into the production Active Directory were: • To ensure that any issues experienced during the pilot were not caused by problems common to the Active Directory production and pilot systems. • To simplify the migration by providing the migration tool with a single scenario in which all users were migrated from Intel's production Active Directory environment.
4-5	Validate new production Active Directory users.	No issues were reported with the migration of users from Windows NT4 domains into the production Active Directory. All production Active Directory user accounts remained active during the pilot as part of a rollback contingency plan.
6	Move the project team to the Active Directory.	All configuration and certification of the pilot environment was completed. Remote access services tests for dial-in and virtual private network (VPN) revealed no problems. The first set of pilot participants were migrated to the pilot Active Directory to provide a final validation of the environment.
7-10	Move all pilot users to the pilot Active Directory and begin the pilot.	The remaining pilot participants were successfully migrated to the pilot Active Directory environment. Pilot users logged into and received services from the pilot Active Directory infrastructure for four weeks.
11	Return all Active Directory pilot users to the production Active Directory.	Moved all users back to production Active Directory. No issues surfaced during this process.

Goal 3 – Maintaining access to resources:

Illustrate how the flexibility of Active Directory's security permits the execution of a pilot in an isolated forest while maintaining each pilot participant's access to all resources on the production network.

From their user accounts and client machines in the ia64.intel.com domain, pilot participants had complete and unrestricted access to all of their resources in the down-level Windows NT 4.0 and Windows 2000 domain infrastructures. There were no problems with trust relationships, SID migration, security access control lists, or sharing resources seamlessly across the different forests and Windows NT 4.0 resource domains. This *clone and trust* technique is Intel's standard methodology for piloting new Active Directory architectures and technologies.

Goal 4 – Porting migration tool

Port internally developed Active Directory migration tools to run on the Itanium architecture as native 64-bit components.

Intel's internally developed user migration tool was quickly and easily ported to the Itanium architecture. Participants were able to access their existing networked resources without any changes to the security access control list, as discussed below,

PILOT STATISTICS

Pilot Users 40

Locations:
- Phoenix, AZ
- Folsom, CA
- Santa Clara, CA
- Hudson, MA
- Hillsboro, OR

Mobile Computers 34
Desktop Computers.....10
Total Computers 44

Itanium-based Authentications 7732
IA-32 Authentications.....283
Total Authentications.....8015

96.5% of the total authentications were serviced by an Itanium-based server.

Porting the Software Tools

Two utility programs, user migration and group synchronization, were used to migrate users to the pilot Active Directory. Both processes applied the *cloning security principals* technology introduced by Microsoft in Windows 2000 Active Directory. *(Security principals* are user accounts, local and global groups, and computer accounts.) User and mirrored group accounts were cloned into the following dedicated organizational units:

User Accounts:
OU=WORKERS, DC=IA64, DC=INTEL, DC=COM

Mirrored Groups:
OU=MIRRORED, OU=GROUPS, DC=IA64, DC=INTEL, DC=COM

User Migration Utility

Intel developed and implemented a Web-enabled user migration application so that users could authenticate their existing Active Directory account and self-migrate to the Itanium-based pilot Active Directory.

Three simple active server pages (ASP) guided the pilot participants through the migration process, making calls to the 64-bit, Out-Of-Proc Visual C++* COM component that is the core engine of the migration utility. This component performs data validation and creates a new, cloned user account in the pilot Active Directory domain. It then uses Microsoft's dsAddSidHistory function to transfer the production and legacy SIDs into the sidHistory property of the newly created account. (The *production* SIDs are the users' SIDs in Intel's production Active Directory; *legacy* SIDs are the SIDs that were stored in the production account's sidHistory property.)

The transfer of production and legacy SIDs enabled users to access any resource (for example, Microsoft Exchange mailbox, file share) that was available to their production (original) Active Directory account. See Figure 2 on the next page for a diagram of the user migration solution stack architecture.

The development platform used to create the user migration tool included:

- Microsoft DevStudio* with Visual C++ 6.0: Development Studio used for editing code.
- Microsoft 64-bit Beta Software Development Kit (SDK): 64-bit SDK and compiler.
- Intel 64-bit SDK Beta version 5.0: 64-bit SDK and compiler.

The execution environment for the tools included:

- Microsoft Whistler-64 (build 2259) 64-bit operating system.

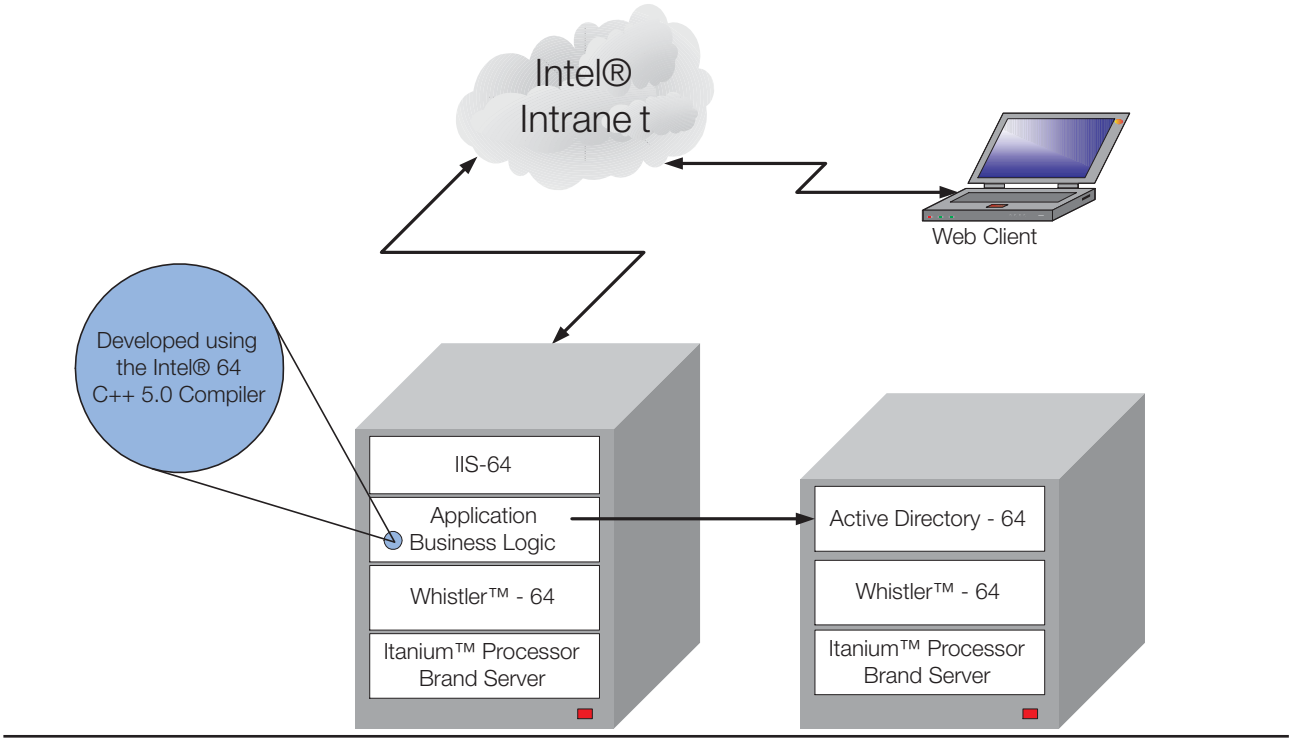

Figure 2. Architecture for User Migration Solution Stack

- 64-bit Internet Information Service (IIS) packaged with Whistler-64 build 2259.
- IE 5.0, packaged with Windows 2000 clients, to provide the user interface for the migration.

Group Synchronization Utility

The group synchronization utility is an Intel-developed 32-bit C++ application designed to synchronize legacy global groups with production Active Directory domains. It uses Microsoft's dsAddSidHistory function call, similar to the User Migration process, to determine users' global groups and mirror them in the Active Directory.

For this pilot, the utility was configured to synchronize legacy global groups with the Itanium-based pilot Active Directory. Once the groups were mirrored, the pilot users were added as members to their respective groups. This allowed each user to access any resource that was granted to a group containing his or her production account.

Conclusion

Intel IT believes that many strategic services—described in the appendix to this document—are enabled by a rapid deployment of Active Directory. As these features come fully into production, the Global Catalog database size is expected to quickly exceed 3 gigabytes. When this occurs, it will be difficult to optimize directory queries that perform full scans of all objects if the entire directory cannot be stored in memory.

Active Directory on Itanium-based servers can help alleviate this problem by implementing strategically-placed domain controllers with enough memory to hold the entire database.

This pilot demonstrates that all layers of the solution stack for Active Directory on an Itanium-based server platform are stable enough to support production services for a pilot user base. Based on the outstanding results of this pilot, Intel IT will continue to work closely with Microsoft and OEM server vendors to prepare for the full implementation of the Itanium-based solution in 2001.

Appendix - Drivers for Deployment of Active Directory

Intel IT took advantage of many of the features in Active Directory to solve key business issues and enable key technologies.

Scalability and Reliability

Intel has grown tremendously in recent years. The Windows NT4 domain architecture has reached practical limits, both in database design and network topology. Active Directory is a highly scalable database engine based on Microsoft's Joint Engine Technology (JET). JET is capable of handling millions of directory objects, and has been proven in Microsoft Exchange Server. This makes Active Directory significantly more

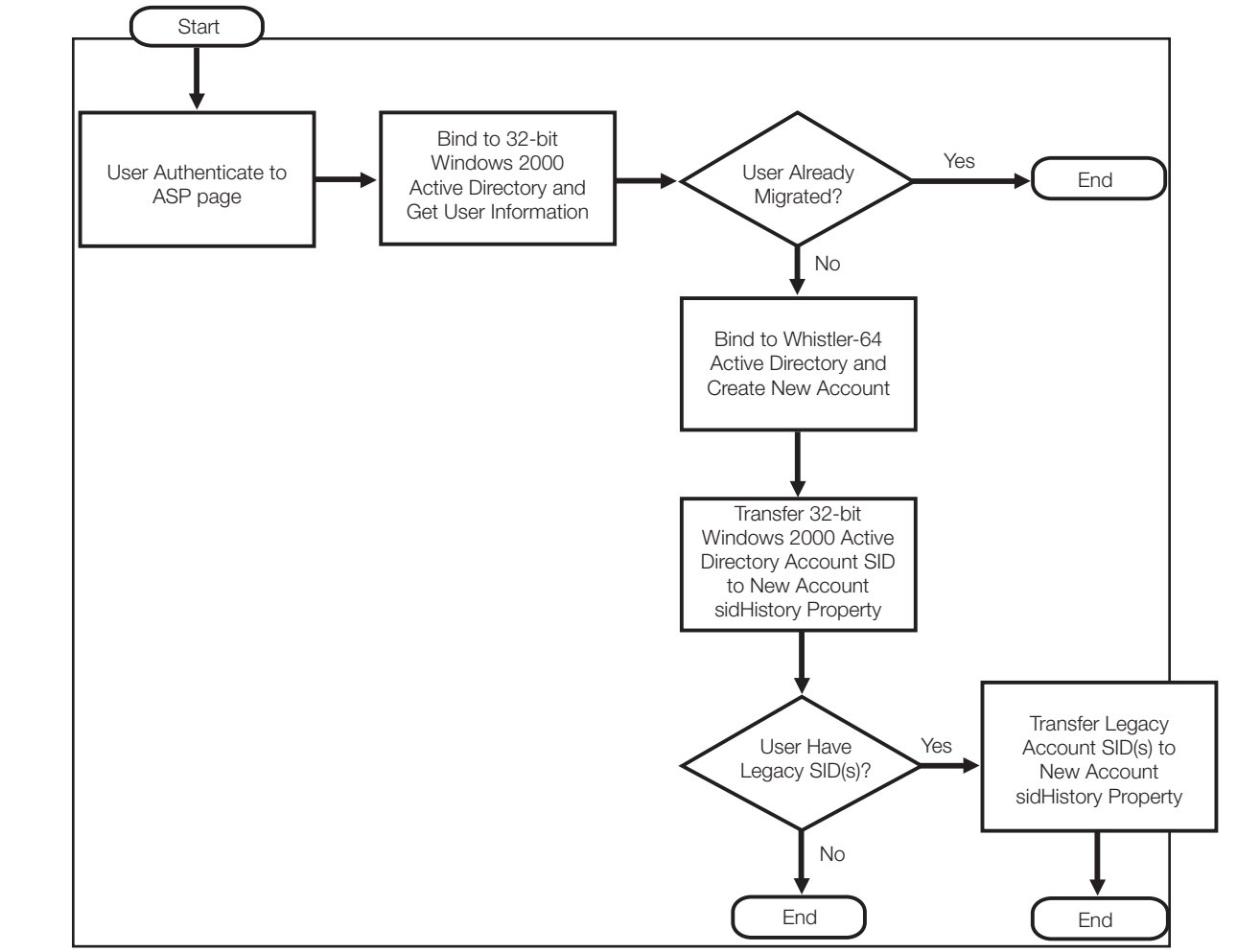

Figure 1. Pilot Trust Architecture

tolerant of critical network outages or periods of network isolation than the NT4 architecture.

Active Directory is a multi-master architecture that permits changes on any domain controller. This enables a physical location to be network-isolated, yet fully capable of executing changes during network outage. The replicated nature of Active Directory also ensures that clients will seamlessly failover to replicas of the Active Directory if any of the Active Directory infrastructure servers fail.

Security Agility

Active Directory uses cloning to enable an Active Directory security principal to retain the security credentials of the original NT security object. This enables, among other things, a smooth upgrade of existing NT-based users, and a far more seamless transition following the acquisition of a corporation that utilizes an NT/Active Directory infrastructure. Similarly, cloning can be used to implement an Active Directory pilot, such as the one described in this paper, where pilot user accounts are cloned from their original into the pilot environment, while retaining access to all of their original resources.

Consolidated Infrastructure

Key infrastructure products such as Microsoft Exchange 2000 can use Active Directory to provide messaging directory services rather than maintaining a separate infrastructure. This consolidation increases the performance load on the Active Directory, as all messaging directory functions (address-book lookups, mail routing, mail configuration) are serviced by the Active Directory infrastructure.

Leverage Internet Standards

Because Active Directory is based on Internet standards, many platforms and operating systems are able to use the security and directory services provided by Active Directory. The primary directory protocol is LDAP, and the primary security protocol is Kerberos, each open Internet standards. Open access to these services enables every application to use the infrastructure, regardless of platform. For example, if a workflow or messaging system executing on Linux* needs access to directory data, it can retrieve it by executing LDAP search calls against Active Directory.

Performance and Security Improvements

Kerberos is a significantly more efficient protocol than NTLM. Its presence enables server-based applications to attain significantly higher scalability. Additionally, Microsoft's implementation of Kerberos permits delegation of authentication, which in turn enables a new breed of N-tier architecture applications.

Public Key Infrastructure

A wide range of encryption, workflow, and security capabilities require an enterprise public key repository. Active Directory provides this capability and enables certificates to be retrieved via the LDAP protocol.

Peer-to-Peer

With the emergence of peer-to-peer technology that leverages all computing resources on a network, directory technology plays an increased role in network management. Critical questions to be answered by an effective peer-to-peer application are "what does the network compute capability look like?" and "where can I find appropriate resources to complete my task?" The directory is very good at answering both of these questions, as it inherently stores a representation of the network capability that can be queried with LDAP to find the best resources to fulfill a task. Furthermore, the extensible schema of Active Directory enables any resource or capability to be represented in the directory as an object.

Directory-Enabled Applications

In addition to peer-to-peer applications, many other critical intranet applications can leverage the distributed data query capabilities of Active Directory. Examples include workflow, human resource, manufacturing, logistics, and engineering.

For more information
To learn more about Intel Corporation, visit our site on the World Wide Web at www.intel.com.

This document and related materials and information are provide "as is" with no warranties, express or implied, including but not limited to any implied warranty of merchantability, fitness for a particular purpose, non-infringement of intellectual property rights, or any warranty otherwise arising out of any proposal, specification, or sample. Intel assumes no responsibility for any errors contained in this document and has no liabilities or obligations for any damages arising from or in connection with the use of this document.

Intel, the Intel logo, Pentium, and Xeon are trademarks or registered trademarks of the Intel Corporation or its subsidiaries in the United States and other countries

*Other names and brands may be claimed as the property of others.

Copyright © 2002 Intel Corporation. All rights reserved.